# IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

## APPLICATION PAPERS

## OF

## ALEXANDER JAMES HINCHLIFFE

## FRASER PETER HOWARD

## ANDREW KEMP

## AND

## BOBBY RAI

## FOR

## MALWARE INFECTION SUPPRESSION

# BACKGROUND OF THE INVENTION

### Field of the Invention

5          This invention relates to the field of data processing systems.   More ·
particularly, this invention relates to suppression of malware, such as computer
viruses and unwanted e-mails, within computer systems

### Description of the Prior Art

10          The threat from malware, such as computer viruses, Trojans, worms and
unwanted e-mails, is increasing.   The consequences of malware infection can be
severe with potential loss of data and system downtime.   Furthermore, the
mechanisms by which malware can spread are becoming more rapid, e.g. internet
connections are increasingly common and e-mail propagated viruses have recently led
15     to a number of rapidly spreading and harmful malware outbreaks.   Measures which
can reduce the problems associated with malware are strongly advantageous.

## SUMMARY OF THE INVENTION

           Viewed from one aspect the present invention provides a computer program
20     product for controlling a computer, said computer program product comprising:
           malware infection detecting logic operable to detect a malware infection of at
least one computer; and
           device disabling logic operable upon detection of said malware infection to
disable operation of one or more data I/O devices of said at least one computer.
25

           The invention recognises that the spreading of malware can be suppressed
when malware infection has occurred by the disabling of I/O devices associated with
the infected computer.   In particular, in order to propagate itself between computers
an item of malware will frequently require the use of an I/O device, such as a floppy
30     disk drive, a removable media drive, a compact disk drive or a network interface card.
Disabling these devices inhibits the ability of the malware to propagate itself and so
reduces the consequences of malware infection.

The disabling of I/O devices may be triggered upon positive identification of a malware infection or more cautiously upon detection of behaviour indicative of malware detection. A more cautious approach is generally better able to deal with newly released malware threats as these may not be able to be positively identified until the malware scanning system has been updated to include tests targeted at those new items of malware. Malware like behaviour could take a variety of forms, but examples would be the sending or receipt of a large number of e-mails bearing the same subject line or having a common attachment.

The malware suppression mechanisms mentioned above may be applied solely to the malware infected computer, or if a more cautious approach is being taken, to further computers even if they are not yet infected. Clearly there is a balance between the disruption caused by disabling the I/O devices of the computers and the disruption caused by potential malware infection.

A complementary aspect of the invention provides a computer program product for controlling a computer, said computer program product comprising:

device disabling logic operable upon receipt by a computer of a command indicative of malware infection precautions being taken to disable operation of one or more data I/O devices of said computer.

It may be that a central computer is responsible for identifying a malware infection or a malware infection is detected by a different client computer, but it is desirable that further computers are able to respond to appropriate commands to disable their I/O devices in order to resist malware infection and propagation.

A further aspect of the invention provides a computer program product for controlling a computer, said computer program product comprising:

user input logic operable to receive a user input indicative of activating precautions against a malware infection; and

device disabling logic operable upon receipt of said user input to disable operation of one or more data I/O devices of said at least one computer.

3

This aspect of the invention allows the I/O disabling action to be taken in response to a manual user input thereby allowing pre-emptive action to be taken to resist malware infection and propagation even if the malware infection has not yet occurred. As an example, a System Administrator may become aware of a rapidly spreading malware threat through media reports or the like and accordingly decide to disable I/O devices as a precaution against potential infection.

Further aspects of the invention provide methods of protecting against malware infection and an apparatus for protecting against malware infection in accordance with the above described techniques.

The above, and other objects, features and advantages of this invention will be apparent from the following detailed description of illustrative embodiments which is to be read in connection with the accompanying drawings.

## BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 schematically illustrates a computer network of a type that may be vulnerable to malware infection;

Figure 2 illustrates various software components within a computer;

Figure 3 is a flow diagram illustrating processing that may be performed by a computer responsible for co-ordinating malware protection;

Figure 4 is a flow diagram illustrating the response of a client computer to a disable command;

Figure 5 is a diagram illustrating the processes by which malware precautions may be triggered semi-automatically; and

Figure 6 is a schematic diagram illustrating a general purpose computer of a type that may be used to implement the above described techniques.

## DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 illustrates a computer network 2 comprising a server 4 and a plurality of client computers 6, 8, 10. In addition a laptop computer 12 may occasionally be connected to the network 2.

The network 2 is vulnerable to malware infection and propagation due to computer viruses and the like being received from removable media 14, such as a floppy disk drive, a zip drive, a Jazz drive, a solid state storage device etc. These removable media may also be passed between users and accordingly propagate infection between computers. A further mechanism by which a malware infection can propagate within the network 2 is via the network interface cards, NICs, associated with each of the client computers 6, 8, 10. File sharing or files stored on the server 4 may propagate the infection, or alternatively e-mails with infected files may be exchanged between network connected computers.

The computer network 2 is connected via the internet to other computer systems and may receive malware infections via its internet connection. The laptop computer 12 may be infected at home, or at another place, and then carry the infection back to the network 2 when it is connected to that network 2 at a later time.

Figure 2 schematically illustrates a number of software components that are typically present within a general purpose computer. An operating system 16 is provided to handle the interface with various physical I/O devices such as a floppy disk drive 18, a compact disk drive 20 and a network interface card 22. In the Windows™ operating system (produced by Microsoft Corporation) a winsoc interface is provided for connecting each of these physical I/O devices 18, 20, 22 to the operating system 16.

Application software need not be directly aware of the configuration and control of the underlying I/O devices 18, 20, 22 as this functionality is carried out by the operating system 16. The application software instead makes API (application program interface) calls to the operating system 16 to instruct the operating system 16 to perform the desired operation. Anti-virus software 24 can operate as such application software and use the operating system 16 to control the input/output devices 18, 20, 22 on its behalf. API calls are provided by the operating system 16 that enable an application

program, such as the anti-virus software 24 to disable and re-enable I/O devices 18, 20, 22. These API calls may be used to disable the I/O devices as required in accordance with the techniques described below.

5      Figure 3 is a flow diagram illustrating the operation of a computer program that serves to co-ordinate and manage at least part of the malware protection of a computer system. An example of such a computer program is Outbreak Manager produced by Network Associates, Inc. This type of co-ordinating computer program can be modified in accordance with the above described techniques to command disabling of I/O devices
10     of specified computers.

At step 26 the system waits until a virus (an item of malware) is detected or virus-like behaviour is detected. Rapid changes in network traffic or the receipt of multiple e-mails containing an identical attachment would be behaviours that could be
15     regarded as virus-like. A virus may also be positively detected via on-access or on-demand scanning mechanisms.

When a virus or virus-like behaviour is detected referencing predetermined rules, processing proceeds to step 28. Depending upon user configured parameters,
20     confirmation of I/O device disablement may be required before this is carried out. If such confirmation is required, then processing proceeds to step 30 where an alert concerning the detected behaviour is displayed to an administrator and their confirmation that I/O device disablement should proceed is sought. If this confirmation is given, then step 32 directs processing to step 34 at which the co-ordinating computer
25     issues I/O device disabling commands to one or more attached computers for which the co-ordinating computer is responsible for managing malware protection. If the disablement is not confirmed at step 32, then the processing terminates. Alternatively, if confirmation was not required at step 28, then processing proceeds directly to step 34.

30     Depending upon user set parameters the response to the detected behaviour may be to disable the I/O devices of only the computer upon which the virus has been detected. The number/type of I/O devices disabled may also be configured. Disablement of I/O devices may extend beyond the computer upon which the infection was detected. In accordance with the principals of operation of Outbreak Manager an

escalating series of responses may be predefined and followed automatically, semi-automatically or manually as a malware outbreak develops.

Figure 4 is a flow diagram schematically illustrating the response of a client computer to commands received from the outbreak manager computer. At step 36 the client computer waits to receive an I/O disablement command. When an I/O disablement command is received, then processing proceeds to step 38 and the anti-virus software 24 issues appropriate API calls to the operating system 16 to disable the selected I/O devices 18, 20, 22.

Figure 5 illustrates another way in which the above described technique may be used. In this case a system administrator becomes aware of a possible virus threat through observing suspicious behaviour of their system, through media reports or through notifications from an anti-virus provider, as well as by other means. If the administrator considers this threat credible, then they may choose to manually trigger disablement of I/O devices, either partially or wholly, upon one or more computers for which they are responsible. This action may be taken as a pre-emptive precaution against infection. An example would be that an administrator may wish to reduce the likelihood of infection at the cost of some inconvenience to their users through the non-availability of their I/O devices until they had confirmed that the potential malware threat was not significant or they had put appropriate other precautions in place, such as downloading the latest virus definition data including a driver for the new malware threat.

When the administrator has selected the I/O device disable option, then the software will automatically trigger the appropriate I/O disable commands to be issued to the client computers specified and those client computers will respond by disabling their I/O devices.

Figure 6 schematically illustrates a general purpose computer 200 of the type that may be used to implement the above described techniques. The general purpose computer 200 includes a central processing unit 202, a random access memory 204, a read only memory 206, a network interface card 208, a hard disk drive 210, a display driver 212 and monitor 214 and a user input/output circuit 216 with a keyboard 218

7

and mouse 220 all connected via a common bus 222. In operation the central processing unit 202 will execute computer program instructions that may be stored in one or more of the random access memory 204, the read only memory 206 and the hard disk drive 210 or dynamically downloaded via the network interface card 208.

5    The results of the processing performed may be displayed to a user via the display driver 212 and the monitor 214. User inputs for controlling the operation of the general purpose computer 200 may be received via the user input output circuit 216 from the keyboard 218 or the mouse 220. It will be appreciated that the computer program could be written in a variety of different computer languages. The computer

10    program may be stored and distributed on a recording medium or dynamically downloaded to the general purpose computer 200. When operating under control of an appropriate computer program, the general purpose computer 200 can perform the above described techniques and can be considered to form an apparatus for performing the above described technique. The architecture of the general purpose

15    computer 200 could vary considerably and Figure 6 is only one example.

Although illustrative embodiments of the invention have been described in detail herein with reference to the accompanying drawings, it is to be understood that the invention is not limited to those precise embodiments, and that various changes and

20    modifications can be effected therein by one skilled in the art without departing from the scope and spirit of the invention as defined by the appended claims.